

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
information associated with)
thememuzickent@gmail.com and/or)
ovathatop01@gmail.com (the "account");)

Case No.22-964M(NJ)

Matter No.: 2022R00300**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 2, 2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

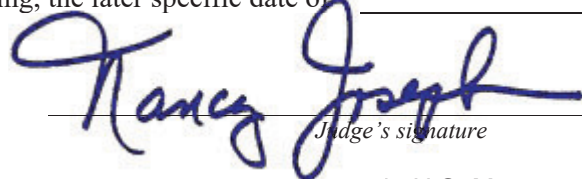
Honorable Nancy Joseph
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 8/18/2022 @ 4:17 p.m.

City and state: Milwaukee, WI



Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with thememuzickent@gmail.com and/or ovathatop01@gmail.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A, from **May 1, 2022, to present:**

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”),

Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) and 18 U.S.C. § 2252A(a)(5)(B) involving the accounts listed in Attachment A since May 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

information associated with thememuzickent@gmail.com
and/or ovathatop01@gmail.com (the "account"); (fully
described in Attachment A)

Case No. 22-964M(NJ)

Matter No.: 2022R00300

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2256(8); § 2256
(2);

Offense Description
Possession, receipt or distribution of child pornography; possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct.

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

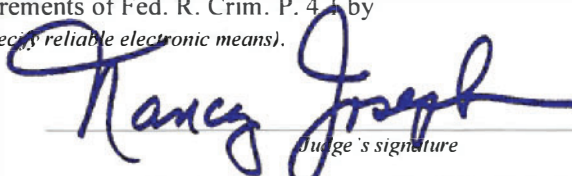
SA Daniel Gartland, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by
_____ telephone _____ (specify reliable electronic means).

Date: 8/18/2022

City and state: Milwaukee, WI



Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
“thememuzickent@gmail.com” and/or
“ovathatop01@gmail.com” THAT IS
STORED AT PREMISES CONTROLLED
BY APPLE, INC.

Case No. __22-964M(NJ)_____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate

violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as “CSAM”).

3. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, contraband and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), which makes it a crime to transport child pornography, and 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography, as described in Attachment B.

DEFINITIONS

6. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B (collectively referred to as “warrant”):

- a. “Child Pornography” is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).
- b. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to “child pornography,” this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); United States v. Riccardi, 258 F.Supp.2d 1212 (D. Kan., 2003) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).
- c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- d. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- e. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- f. “Electronic device” includes any electronic, magnetic, optical, electrochemical or other high speed system or device capable of storing and/or processing data in digital form, including but not limited to the following: central processing units; desktop, laptop, and notebook computers; tablets; PDAs; wireless communication devices such as cellular telephones and pagers; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, routers, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, flash drives, magnetic tapes and memory chips; security devices; and any

data storage facility or communications facility directly related to or operating in conjunction with such device.

- g. “Hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to hardware (including physical keys and locks).
- h. “Software” is digital information which can be interpreted by an electronic device and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- i. “Electronics-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use hardware, software, or other related items.
- j. “Passwords and data security components” consist of information or items designed to restrict access to or hide software, documentation, or data. Data security components may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters or symbols) usually operates a sort of digital key to “unlock” data security components. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- k. “Internet Service Providers” (ISPs) are commercial organizations, which provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means to access the internet, including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, fiber optic cable, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox. The subscriber is then typically required to create a password for the account. By using an internet-capable electronic device, the subscriber and other

users can establish digital communication with an ISP and thereby access the internet.

- l. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.
- m. “Internet Protocol address” (IP address) refers to a unique number used by an electronic device to access the internet. IP addresses can be dynamic, meaning the Internet Service Provider (ISP) assigns a different unique number to an electronic device every time it accesses the internet. IP addresses are considered static if an ISP assigns a user’s electronic device a particular IP address, which is used each time the device accesses the internet.
- n. The terms “records,” “documents” and “materials” include all information recorded in any form, visual or audio, and by any means, whether in hand-made form (including writings, drawings, painting); photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including phonograph records, printing, typing); or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators; and digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- o. “Image” or “copy” refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but certain attributes may change during the reproduction.
- p. “Log Files” are records automatically produced by software to document electronic events that occur on electronic devices. Software can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote electronic devices; access logs list specific information about when an electronic

device was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- q. “Cellular telephones” are handheld electronic devices used for wireless voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- r. “Emojis” are small digital images or icons used in electronic messages or webpages to communicate an idea, emotion, expression, or feeling. Emojis exist in various genres, including facial expressions, common objects, places, types of weather, and animals.

**BACKGROUND ON ELECTRONIC DEVICE USE IN FACILITATING
CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION CRIMES**

7. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

- a. Electronic devices and related technology have revolutionized the way in which child pornography is produced, distributed, viewed, and stored, as well as how it is used in furtherance of online child exploitation.
- b. Individuals can convert photographs and videos taken using a traditional camera or video recorder to a format capable of being disseminated quickly and efficiently via the internet using a variety of electronic devices, including scanners, memory card readers, cellular telephones, or directly from digital cameras.
- c. Modems and routers allow electronic devices to connect to other devices using telephone, cable, or wireless connections. Electronic contact can be made to literally millions of devices around the world.

- d. The capability of electronic devices to store extremely large amounts of high-resolution video and imagery in digital form, which can be password protected or hidden from other device users, makes these devices highly effective at storing child pornography, while also concealing the user's illicit activity.
- e. The internet affords individuals many different and relatively secure and anonymous venues for obtaining, viewing, and distributing child pornography; or for communicating with others to do so; or to entice children.
- f. Individuals can use online resources to retrieve, store and share child pornography, including services offered by internet portals such as Google, Yahoo!, and Facebook, among others. Online services, which are accessed via electronic device, generally allow a user to set up an account which thereby provides the user with access to email, instant messaging services, online file storage, social media, online message boards, and/or a variety of other interconnected web-based applications. If a user uses any of these functions to obtain, view, store, or distribute child pornography; or for communicating with others to do so; or to entice children, evidence of such activity can often be found on the user's electronic device.
- g. As is the case with most digital technology, electronic device communications can be saved or stored on hardware and digital storage media. Storing this information can be intentional, i.e., by saving an e-mail as a file on the electronic device or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic device user's internet activity generally leaves traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.
- h. The interaction between software and the electronic device's operating systems often results in material obtained from the internet being stored multiple times, and even in different locations in the device's digital memory, without the user's knowledge. Even if the device user is sophisticated and understands this automatic storage of information, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the digital media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's digital media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution, and/or possession of child pornography.

- i. Data that exists on an electronic device is particularly resilient to deletion. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on most electronic devices, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user’s operating system, storage capacity, and device habits.

PROBABLE CAUSE

8. On May 9, 2022, the National Center for Missing and Endangered Children (NCMEC) received information from Dropbox, Inc. (Dropbox) that suspected Child Sexual Abuse Material (CSAM) was uploaded to the Dropbox account belonging to user Brandon Gilmore. The following user information was provided:

- a. Email address: **thememuzickent@gmail.com**
- b. Screen/username: Brandon Gilmore

9. Dropbox provided six videos uploaded to the account associated with user Brandon Gilmore. NCMEC provided the information to the Federal Bureau of Investigation for further action. The first video showed a female removing her clothes and touching her vagina. The video then showed an adult male touch her vagina and engaged in vaginal and anal sex with the female. The female appeared to be in the early stages of puberty with minor breast development and some

pubic hair. The second video showed adult male engaged in vaginal sex with a minor female. The female appeared to be pre-pubescent, lacking pubic hair and breast development. The third video showed an adult male engaged in oral sex with a minor female. The female wore a blindfold over her eyes. The words, “suck cock cum slut” were written on the blindfold. The female had facial features consistent with a pre-pubescent child. The fourth video showed a close-up view of an adult male engaged in vaginal sex with a pre-pubescent female, lacking pubic hair. The fifth video depicted an adult male laying on a bed while two unclothed females removed his pants and touched his penis and testicles. The females appeared to be pre-pubescent, lacking breast development and pubic hair. The sixth video showed a female sitting on a chair with her pants pulled down. An adult male then lifted her legs displaying her anus and vagina. The video then showed the male spreading open the minor female’s vagina. The female appeared to be pre-pubescent, lacking breast development and pubic hair. The female also wore a t-shirt with a cartoon drawing of a smiling sun. An upload log provided by Dropbox indicated the videos were uploaded on or about May 7, 2022.

10. On June 6, 2022, Dropbox provided information in response to a subpoena requesting user account information and IP addresses associated with the Dropbox user Brandon Gilmore. The information revealed that the account was accessed by IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e on May 7, 2022.

11. Further investigation determined that the IP address 2600:1700:9434:6190:40dd:39d3:ced6:f56e was assigned to an AT&T account with the following subscriber information:

- i. Account Number: 314010876
- ii. Subscriber Name: Brianna Roeck

iii. Account Creation: 06/11/2021

iv. Service Address: 3640 South 87th Street, Milwaukee, WI, 53228

12. A search of law enforcement databases revealed that in June of 2021 Brandon Gilmore (XX/XX/1989) was involved in a vehicular accident in Milwaukee, WI, while driving a black Chevrolet Equinox bearing Wisconsin registration plate ACS-3373 (hereinafter “Equinox”). The registered owner of the Equinox was Brianna Roeck. Gilmore also owns a blue 2004 Chevrolet Impala registered with the state of Wisconsin at the address 3640 South 87th Street, Milwaukee, WI.

13. On July 25, 2022, Special Agents with the Federal Bureau of Investigation (FBI) observed Brianna Roeck arrive at 3640 South 87th Street, Milwaukee, WI, driving the Equinox. Agents observed Gilmore leave the address and return while driving the Equinox. Agents also observed a blue Impala without visible plate parked at the address.

14. An open-source search of Facebook revealed a profile with the name, “Brianna Röck.” The profile includes references to the “Gilmore’s” and includes photos that appear to show Brianna Roeck and Brandon Gilmore together. The profile also contains references to Brynlee Gilmore, a baby born in early-October 2021 and photos of two other female children. Based upon the information in the Facebook profile, I believe Brianna Roeck and Brandon Gilmore are in a relationship.

15. A search of law enforcement databases revealed that Brandon Gilmore is a registered sex offender and resides at the address 3640 South 87th Street, Milwaukee, WI. On July 23, 2013, Gilmore was arrested by the FBI in Minneapolis, MN for a violation of Title 18 U.S.C. § 2423 (d) and (e) Conspiracy to Facilitate in Transportation of Minors for Prostitution. The arrest was the result of an investigation into Gilmore and two other females for the transportation of a

14-year-old female from Milwaukee, WI to Bloomington, MN for the purpose of engaging in prostitution. Gilmore plead guilty to the charge and was sentenced to 82 months in federal prison and 60 months of supervised release. Gilmore remained on supervision with the United States Probation Office for the Eastern District of Wisconsin as of July 26, 2022 and was due to complete his supervision on August 13, 2024.

16. On July 27, 2022, a search warrant, issued in the United States District Court for the Eastern District of Wisconsin on July 27, 2022, was executed by the FBI at 3640 South 87th Street, Milwaukee, WI. During the search, law enforcement officers seized as evidence an Apple iPhone 13 with serial number: DPQ00N306, (hereinafter, “the Phone”) from the location. Pursuant to the search warrant, a forensic examination of the phone. The was assigned telephone number 414-708-5314 and had an Apple ID associated with the e-mail address, **thememuzickent@gmail.com**.

17. The Phone appeared to have an initial power on date of June 26, 2022. The phone included data from dates prior to the initial power on date. Based on my training and experience, I believe the user of the phone obtained a new device on or about June 26, 2022 and synced the Phone with data maintained in on an external cloud-based server.

18. The phone contained several social media accounts and associated conversations. A Facebook profile and Facebook Messenger account on the phone was associated with the username Charles Palmer with the identification number 10006618555099. A Kik messenger account with a username of “bgillie08” and the e-mail address, **Ovathatop01@gmail.com**. The Apple wallet for the Phone was associated with “Brandon Gilmore” at the address 4597 North Houston Avenue, Milwaukee, WI. Law enforcement databases indicate that 4597 North Houston Avenue, Milwaukee, WI is the address of Tequila Matthews, mother of Brandon Gilmore.

19. Investigators conducted a review of Kik messenger conversations recovered from the telephone. At least two conversations contained discussions of Child Sexual Abuse Material (CSAM). On July 17, 2022, Kik user “claraoglyta_cb5” (hereinafter, “CB5”) initiated a conversation with the account associated with the phone. CB5 asked “Are you a buyer of cp mega link and video?” CB5 further provided an apparent list of the types of CSAM available. Bgillie08 responded “Samples.” A link to at least one video of suspect CSAM was sent to Bgillie08 and a request for payment was made. On July 25, 2022, Bgillie08 messaged “Samples” to Claraoglyta_cb5, though the message did not appear to be delivered.

20. A Kik conversation between bgillie08 and dirtydaughter101_n1k (hereinafter, “N1K”) occurred from July 17, 2022 to July 25, 2022. The conversation began with N1K sending links of known or suspected CSAM to Bgillie08 and a request to “Send me the screenshot baby.” Bgillie08 responds with a screenshot of a \$50 payment via an electronic funds transfer application to a user named “Malacia Hyche.” Bgillie08 then messages, “Penetration and cum” and “And anal.” N1K then provided additional videos. Bgillie08 later states, “I’ll send more money when I have all 50 videos u promised for the 30 I sent.” After receiving a series of videos, Bgillie08 states, “That’s not cp. That don’t count.” Further videos and requests for money were sent from N1K until July 19, 2022. On July 25, 2022, the conversation ended with Bgillie08 asking, “Samples?”

21. Investigators conducted a review of the images and videos recovered from the Phone. The phone contained numerous selfie-style images of Brandon Gilmore, including metadata with a location in the area of 3640 South 87th Street, Milwaukee, WI. The phone contained approximately 34 videos of known or suspected CSAM. Five of these videos are further described as follows:

- A close-up video of an infant, approximately less than one year of age, with a white

fabric background. The child did not appear to have developed lower teeth. The child's bare chest was visible in the video. The child appeared to be Caucasian, though hair color and sex of the child could not be determined based upon the view of the camera. An erect adult penis was inserted into the child's mouth during the video. The video appeared to have been recovered from applications on the Phone.

- A video of a pre-pubescent female, approximately four to eight years of age, laying on her back with her legs held up. The female had short dark brown or black hair and a light skin tone. The child did not have developed breasts or pubic hair. The child's mannerisms were consistent with a mental handicap. Written on the inner thigh of the child's left leg is the letter "I", a drawing of a heart and an illegible word. The female child was completely naked, and her anus and vagina were clearly visible. There was apparent male ejaculate on the child's legs, vagina and seeping from her anus. A white-skinned adult hand with manicured fingernails pointed to the ejaculate in the child's anus. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately five to nine years of age, visible from the mid-torso down. The child was light skinned. Her face and hair were not visible in the video. The female was wearing a pink and white striped bathing suit with a pink and blue flowers or starfish pattern. The child's bathing suit was pushed to the side and her vagina was partially visible. A white skinned adult male penis had vaginal sex with the child. The adult male's right hand was pressed down on the child's stomach area. The video appeared to have been recovered from applications on the Phone.

- A video of a pre-pubescent female, approximately five to nine years of age, standing in front of a white skinned adult male. The female child is light skinned with short brown hair. The female was wearing a white T-shirt and did not appear to be clothed from the waist down. The female did not appear to have developed breasts. The adult male was wearing a white T-shirt pulled up above his belly button. The adult male has the child perform oral sex on him. The adult male had one hand on the child's shoulder and the other hand manipulated the zoom on a camera with a remote. The video appeared to have been recovered from applications on the Phone.
- A video of a pre-pubescent female, approximately two to six years of age, lying on a carpeted floor. The child was light skinned. The child did not have pubic hair. Her face and hair were not visible in the video. The child appeared to be wearing a green T-shirt, pulled up above her chest. The child's vagina was clearly visible in the video. A dark-skinned adult male with an erect penis had anal and vaginal sex with the child before ejaculating on the child's pubic area. The adult male held the child down at various points in the video by gripping the child's waist. The video appeared to have been recovered from applications on the Phone.

22. On July 27, 2022, Brandon Gilmore was interviewed by Special Agents of the FBI in a non-custodial setting at the FBI Milwaukee Field Office. During the interview, Gilmore stated that he had a Dropbox account when he was first released from prison. The account was registered with the e-mail address **thememuzickent@gmail.com**. Gilmore maintained a few self-developed rap songs on the account and had not used it in several years. Gilmore also used the e-mail address **ovathatop01@gmail.com**. Gilmore provided the pass code to his phone and stated that he did not

have Dropbox on the phone. He further stated that there was not child pornography on his phone. Gilmore stated he “was not concerned about child pornography” and “did not watch child pornography.”

INFORMATION REGARDING APPLE ID AND iCloud

23. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

24. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple

devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

25. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

26. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

27. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

28. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

29. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

30. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by

Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

31. A device linked to the Apple account contained CSAM. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

32. The investigation has included the transportation of CSAM from a device to a Dropbox cloud storage account. Those same methods could be used to transport CSAM from a device to cloud storage accounts associated with an iCloud Drive. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses

under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

33. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

34. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to

communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

36. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

38. Based on the forgoing, there is probable cause to believe that Brandon Gilmore is utilizing or has utilized his Dropbox account in violation of Title 18 U.S.C. § 2252A, which, among other things, makes it a federal crime for any person to possess, receive, transport, or distribute child pornography, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located in the Apple iCloud associated with the Apple ID thememuzickent@gmail.com and/or ovathatop01@gmail.com.

39. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with thememuzickent@gmail.com and/or ovathatop01@gmail.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A, from **May 1, 2022, to present:**

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”),

Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) and 18 U.S.C. § 2252A(a)(5)(B) involving the accounts listed in Attachment A since May 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **[PROVIDER]**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **[PROVIDER]**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature